UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DAVID STERN, CYRUS JENANI, and DANIEL SOFFER, Individually and on behalf of all others similarly situated, Plaintiffs, v. SCOTTRADE, INC., a Missouri Corporation, Defendant.	)	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs David Stern ("Plaintiff Stern"), Cyrus Jenani ("Plaintiff Jenani"), and Daniel Soffer ("Plaintiff Soffer" and, collectively, "Plaintiffs") bring this class action individually and on behalf of all others similarly situated against Scottrade, Inc. ("Scottrade" or the "Defendant"). Plaintiffs make the following allegations upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by their attorneys, and state as follows:

NATURE OF THE ACTION

1. Beginning in or around late 2013 and continuing through early 2014, Scottrade's confidential database was hacked, leaving millions of Scottrade consumers exposed to fraud and identity theft. Cybercriminals accessed personal information, such as names, addresses, social security numbers, email addresses, and financial information, from approximately 4.6 million consumers.

2. The data breach is a direct result of Scottrade's negligent failure to implement and maintain reasonable and industry-standard security measures to protect its consumers' personal and financial information. Scottrade's failure to safeguard its database is even more egregious

considering this is not the first time Scottrade has been criticized for having weak security measures. Recently, in 2014, a hacker accessed retail brokerage accounts and made unauthorized trades in Scottrade. Moreover, in 2013, FINRA fined Scottrade for failing to implement and have in place a reasonable supervisory system.

3. Despite the fact that the security breach initially occurred nearly two years ago, Scottrade has only recently begun to notify its consumers of the breach. The notice sent to Scottrade customers, however, is also deficient, failing to fully explain the nature and cause of the massive data breach.

4. Plaintiffs bring this class action lawsuit on behalf of Scottrade customers whose personal and financial information has been compromised as a result of the data breach. Plaintiffs seek injunctive relief requiring Scottrade to implement and maintain security practices that comply with regulations designed to prevent and remedy these types of breaches, as well as restitution, damages, and other relief.

JURISDICTION AND VENUE

5. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs and there are more than 1,000 members of the Class (as defined below). Further, Plaintiff David Stern, a citizen of New York, Plaintiff Daniel Soffer, a citizen of New Jersey, and Plaintiff Cyrus Jenani, a citizen of California, and many Class members are citizens of a different state than the Defendant, which is incorporated in Missouri and has its principal place of business in Missouri.

6. This Court has personal jurisdiction over Scottrade because Scottrade is authorized to conduct business in New York and transacts substantial business in this District through its retail

stores within New York. Scottrade, thus, has sufficient minimum contacts with New York to render exercise of jurisdiction by this Court in compliance with traditional notions of fair play and substantial justice.

7. Venue is proper in this District pursuant to 28 U.S.C. § 1391 (a)-(d) because, *inter alia* Scottrade regularly transacts business in this District and a substantial part of the events giving risk to this cause of action took place in this District.

PARTIES

8. Plaintiff David Stern is an individual residing in New York. Plaintiff Stern opened an account with Scottrade on or about June 27, 2005. Believing Scottrade would safeguard his personal information, Plaintiff Stern provided his confidential and highly sensitive personal and private information to Scottrade during the enrollment process. On or about October 7, 2015, Plaintiff Stern received a letter from Scottrade via email informing Stern "about a security compromise involving a database containing some of [Stern's] personal information."

9. Plaintiff Daniel Soffer is an individual residing in New Jersey. Plaintiff Soffer opened an account with Scottrade approximately fifteen (15) years ago. Believing Scottrade would safeguard his personal information, Plaintiff Soffer provided his confidential and highly sensitive personal and private information to Scottrade during the enrollment process. On or about October 7, 2015, Plaintiff Soffer received a letter from Scottrade via email informing Soffer "about a security compromise involving a database containing some of [Soffer's] personal information." Subsequent to the data breach, numerous attempts were made to open lines of credit using Soffer's data.

10. Plaintiff Cyrus Janani is an individual residing in California. Plaintiff Janani opened an account with Scottrade at a date unknown but prior to 2014. Believing Scottrade would

safeguard his personal information, Plaintiff Janani provided his confidential and highly sensitive personal and private information to Scottrade during the enrollment process. On or about October 2, 2015, Plaintiff Janani received a letter from Scottrade via email informing Janani "about a security compromise involving a database containing some of [Janani's] personal information."

11. Defendant Scottrade is a Missouri corporation with its principal executive offices located in St. Louis, Missouri.

FACTUAL BACKGROUND

I. SCOTTRADE MARKETS ITSELF AS A TRUSTWORTHY COMPANY WITH PROTECTIVE POLICIES IN PLACE TO SAFEGUARD CONSUMERS' PERSONAL INFORMATION

12. Opening in 1980, Scottrade is a privately owned discount retail brokerage firm with over 500 branch offices in the United States. Scottrade renders both online and branch office services, including brokerage services, banking services, investment education, and online trading platforms.

13. In order to create a Scottrade investment account, customers must provide certain personal and confidential information to Scottrade during the sign up process.[1] This information includes names, addresses, phone numbers, social security numbers, employment information and other personal information.

14. Scottrade's Privacy Statement explains to consumers that their personal information may also be collected from third parties: "We also collect your personal information from others, such as credit bureaus, affiliates or other companies."[2]

---

[1] https://www.scottrade.com/documents/alt/PrivacyStatement.pdf (last visited Oct. 23, 2015).

[2] *Id.*

15. Scottrade markets and holds itself out as a company that can be trusted by consumers and the public at large. It assures its consumers that as a result of its "continued stability and steady growth . . . [its] clients have been empowered to invest with confidence."[3] According to Scottrade's Privacy Statement, the Company assures customers that Scottrade vigorously protects the private and confidential information of its customers:

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.[4]

16. Scottrade also makes a number of representations on its website regarding its concern for the protection of its customers' personal information and the steps Scottrade takes to safeguard that information. For example, under a page titled "Secure Online Investing & Identity Theft Protection," Scottrade represents, in part, the following:

> **Take Control of Your Safety**
>
> At Scottrade, we take security seriously and use a variety of measures to protect your personal information and accounts. We keep all customer information confidential and maintain strict physical, electronic and procedural safeguards to protect against unauthorized access to your information.
>
> Scottrade is committed to constantly updating its practices to stay ahead of identity thieves. Using VeriSign Identity Protection Fraud Detection Service, for example, Scottrade automatically checks your account for signs of activity from a foreign computer.[5]

---

[3] https://www.scottrade.com/online-brokerage/company-overview.html (last visited Oct. 23, 2015).

[4] *Id.*

[5] https://www.scottrade.com/online-brokerage/secure-trading.html (last visited Oct. 23, 2015).

17. Viewing Scottrade as a trustworthy company is important to consumers, since their personal information—including social security numbers, names, addresses, and financial information—is entrusted in Scottrade and stored on Scottrade's network.

18. Scottrade recognizes the importance of protecting its customers' highly sensitive and valuable information, as well as the dire consequences of falling victim to identity theft if such information is accessed by unauthorized third parties. In fact, Scottrade warns its customers that "Identity theft is the theft of your personal information, which is then used to commit fraud. Account numbers, Social Security numbers and other pieces of personal information can all be used to commit fraud."[6] Scottrade describes how it protects against identity theft:

> **How We Protect You**
> Awareness is critical. That's why we've developed these guidelines:
>
> **Identify Theft Schemes**
> Arm yourself against an attack by learning about potential threats.
>
> 1. **Phishing** is a scheme to collect personal information via e-mail or pop-ups which seem legitimate. Pharming is a hacker's attempt to redirect a website's traffic to another, bogus website. Both are common ways hackers collect personal information.
>
> 2. **Trojan horse -** a program that installs bad code that's hidden or harmless until an action occurs, such as clicking a link. When this happens, a hacker can access your keystrokes to get passwords or other personal information. Trojan horses are spread through e-mail or embedded in Web pages, spyware, and worms via "free downloads."
>
> 3. **Detect spyware –** keep your operating system updated by enabling the automatic Windows updates or by downloading Microsoft updates regularly. It's the best defense against spyware installation.[7]

---

[66] *Id.*

[7] https://www.scottrade.com/online-brokerage/secure-trading/security-center.html (last visited Oct. 23, 2015).

19. At all relevant times, Scottrade had the above privacy policy in effect and made such representations to Plaintiffs and the Class. Plaintiffs and the Class bargained for the privacy and security of their information during the sign up process and through their customer agreement with Scottrade. The security of Plaintiffs' personal and financial information was central to their decision to invest in Scottrade.

II. THE DATA BREACH

20. On October 1, 2015, Scottrade disclosed through its website that its network had been hacked, compromising the records of approximately 4.6 million customers.[8] Specifically, between late 2013 and early 2014, cybercriminals hacked into Scottrade's network and stole client names and street addresses. The cybercriminals had access to customers' social security numbers, email addresses and other sensitive data but, according to Scottrade, "it appears that contact information was the focus of the incident."[9]

21. According to Scottrade's website, it did not become aware of the breach until it was contacted by Federal law enforcement officials.[10] Brian Krebbs ("Krebbs"), a respected security blogger, contacted Scottrade to inquire about the context of the notification the company received. In response, "Scottrade spokesperson Shea Leordeanu said the company couldn't comment on the incident much more than the information included in its Web site notice about the attack. But she did say that Scottrade learned about the data theft from the Federal Bureau of Investigation ("FBI"), and that the company is working with agents from FBI field offices in Atlanta and New York. FBI officials could not be immediately reached for comment."[11]

---

[8] https://about.scottrade.com/updates/cybersecurity.html (last visited Oct. 23, 2015).

[9] *Id.*

[10] *Id.*

[11] Brian Krebs, Scottrade Breach its 4.6 Million Customers (Oct. 2, 2015),

22. According to Krebbs, the data stolen may have been taken to facilitate stock scams, similar to what happened in the 2014 data breach involving JPMorgan Chase.[12] The authorities in the JPMorgan Chase investigation suspect that the stolen email addresses were used to further stock manipulation schemes involving spam emails to pump up the price of otherwise worthless penny stocks.[13] It is speculated that the same motivation could be at the heart of the Scottrade data breach.

23. According to a December 22, 2014 New York Times article, entitled "Neglected Server Entry for JPMorgan Hackers, the attack on J.P. Morgan was preventable:

> Most big banks use a double authentication scheme, known as a two-factor authentication, which requires a second one-time password to gain access to a protected system. But JPMorgan's security team had apparently neglected to upgrade one of its network servers with the dual password scheme, the people briefed on the matter said. That left the bank vulnerable to intrusion.
>
> * * *
>
> The revelation that a simple flaw was at issue may help explain why several other financial institutions that were targets of the same hackers were not ultimately affected nearly as much as JPMorgan Chase was. To date, only two other institutions have suffered some kind of intrusion, but those breaches were said to be relatively minor by people briefed on the attacks.
>
> What is clear is JPMorgan's attack did not involve the use of a so-called zero day attack — the kind of sophisticated, completely novel software bug that can sell for a million dollars on the black market. Nor did hackers use the kind of destructive malware that government officials say hackers in North Korea used to sabotage data at Sony Pictures.
>
> * * *
>
> It is not clear why the vulnerability in the bank's network had gone unaddressed previously. But this summer's hack occurred during a period of high turnover in

---

http://krebsonsecurity.com/2015/10/scottrade-breach-hits-4-6-million-customers/.

[12] *Id.*

[13] *Id.*

the bank's cybersecurity team with many departing for First Data, a payments processor.

III. THE INADEQUATE AND DELAYED NOTIFICATION TO THE CLASS

24. On October 2, 2015, Scottrade began notifying Plaintiffs and the Class about the data breach. The notification, which was sent via email, states, in relevant part:

> Dear Client:
>
> We are writing to share with you important information about a security compromise involving a database containing some of your personal information, as well as steps we are taking in response, and the resources we are making available to you.
>
> **What Happened**
>
> Federal law enforcement officials recently informed us that they've been investigating cybersecurity crimes involving the theft of information from Scottrade and other financial services companies. We immediately initiated a comprehensive response.
>
> Based upon our subsequent internal investigation coupled with information provided by the authorities, we believe a list of client names and street addresses was taken from our system. Importantly, we have no reason to believe that Scottrade's trading platforms or any client funds were compromised. All client passwords remained encrypted at all times and we have not seen any indication of fraudulent activity as a result of this incident.
>
> Although Social Security numbers, email addresses and other sensitive data were contained in the system accessed, it appears that contact information was the focus of the incident.
>
> The unauthorized access appears to have occurred over a period of several months between late 2013 and early 2014. We have secured the known intrusion point and conducted an internal data forensics investigation on this incident with assistance from a leading computer security firm. We have taken appropriate steps to further strengthen our network defenses.
>
> **What Happens Now**
>
> Federal authorities had requested that they be allowed to complete much of their investigation before we notified clients. In coordination with them, we are now able to alert you of this incident. We are fully cooperating with law enforcement in their investigation and prosecution of the criminals involved.
>
> Notices like this one are being sent to all individuals and entities whose information was contained in the affected database, and we have included here information about steps

you can take to protect yourself.

25. Scottrade's email continues, making it clear that the onus is on Plaintiffs and Class members, rather than Scottrade, to protect themselves and mitigate against any damages caused by the data breach:

> **What You Can Do**
>
> As always, we encourage you to regularly review your Scottrade and other financial accounts and report any suspicious or unrecognized activity immediately. As recommended by federal regulatory agencies, you should remember to be vigilant for the next 12 to 24 months and report any suspected incidents of fraud to us or the relevant financial institution. Please also read the important information included on ways to protect yourself from identity theft.
>
> We encourage clients to be particularly vigilant against email or direct mail schemes seeking to trick you into revealing personal information. Never confirm or provide personal information such as passwords or account information to anyone contacting you. Please know that Scottrade will never send you any unsolicited correspondence asking you for your account number, password or other private information. If you receive any letter or email requesting this information, it is fraudulent and we ask that you report it to us at phishing@scottrade.com. Be cautious about opening attachments or links from emails, regardless of who appears to have sent them.

26. The email also states that Scottrade will provide one year of free credit monitoring to its customers:

> **Identity Theft Protection**
>
> As a precaution, Scottrade has arranged with AllClear ID to help you protect your identity at no cost to you for a period of one year. You are pre-qualified for identity repair and protection services and have additional credit monitoring options available, also at no cost to you.
>
> You can call AllClear ID with any concerns about your identity at 855.229.0083. This hotline is available from 8:00 am to 8:00 pm (central) Monday through Saturday.
>
> We have also included additional steps you could consider at any time if you ever suspect you've been the victim of identity theft. We offer this out of an abundance of caution so that you have the information you need to protect

> yourself.
>
> We are very sorry that this happened and for any uncertainty or inconvenience this has caused you. We know that incidents like these are frustrating. We take the security of your information very seriously and are committed to continually strengthening and evolving our defenses based on new and emerging threats.
>
> Sincerely,
> Scottrade

27. Scottrade's offered "credit monitoring," however, is inadequate and requires Plaintiffs and the Class to spend additional time and resources just to set the monitoring up. Furthermore, the credit monitoring offered by Scottrade, AllClear ID, is completely inadequate. As described by one news source:

> [AllClear ID] while a popular choice for companies like Scottrade to provide complimentary protection to customers in the event of a data breach, does not offer the best protection a consumer could have. Specifically, it is missing two crucial features that make one of these services effective: Internet black market monitoring and access to your triple-bureau credit reports and scores.[14]

28. Thus, Scottrade's offered credit monitoring is a haphazard effort to address concerns by those affected by the breach, but in reality it does not provide the quality of coverage necessary to monitor for identity theft. Rather, Plaintiffs and the Class are left to incur the costs of finding adequate credit and identity theft monitoring.

29. The email proceeds to outline additional precautions Scottrade customers can take to protect against identity fraud, all of which require additional time and expenses that would be incurred by Plaintiffs and the Class:

> **Important Identity Theft Information: Additional Steps You Can Take to Protect Your Identity**

[14] Jocelyn Baird, 4.6 Million Customers Affected in Scottrade Breach: Are You One of Them? (Oct. 6, 2015), http://www.huffingtonpost.com/nextadvisorcom/46-million-customers-affe_b_8248276.html.

The following are additional steps you may wish to take to protect your identity.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies.

You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll-free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

- Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com

- Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742. www.experian.com

- TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. www.transunion.com

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1.800.525.6285
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.680.7289

Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing

> or other services. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00 each to place, temporarily lift, or permanently remove a security freeze.
>
> To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the following addresses:
>
> - Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348
> - Experian Security Freeze, P.O. Box 9554, Allen, TX 75013
> - TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

30. The email sent out by Scottrade is also deficient in that it fails to explain the breadth of the breach and the potential threat that consumers face. For example, the email does not explain why or how the breach occurred, the number of people impacted, or why this information was not properly safeguarded. It furthermore fails to explain what information was actually taken during the breach. Although it states that "contact information was the focus of the incident," it does not explain why the other sensitive information in the database, such as social security numbers, is not believed to have been taken.

31. Many affected customers, however, will not even receive this email, since they may have changed email addresses or used alternative email addresses for personal and financial matters.

IV. SCOTTRADE KNEW ITS SECURITY SYSTEM WAS INADEQUATE

32. Exacerbating matters, Scottrade was on notice of its flawed security system as early as 2011, as it has been fined and criticized on several occasions for its weak network security and lack of supervisory mechanisms. For instance, FINRA recently fined Scottrade $300,000 for failing to implement reasonable supervisory systems:

> The Financial Industry Regulatory Authority (FINRA) announced today that it has fined Morgan Stanley Smith Barney, LLC (Morgan Stanley)

> $650,000 and Scottrade, Inc. $300,000 for failing to implement reasonable supervisory systems to monitor the transmittal of customer funds to third-party accounts. Both firms were cited for the weak supervisory systems by FINRA examination teams in 2011, but neither took necessary steps to correct the supervisory gaps.
>
> Brad Bennett, Executive Vice President and Chief of Enforcement, said, "Firms must have robust supervisory systems to monitor and protect the movement of customer funds. Morgan Stanley and Scottrade had been alerted to significant gaps in their systems by FINRA staff, yet years went by before either firm implemented sufficient corrective measures."
>
> * * *
>
> FINRA also found that Scottrade failed to establish a reasonable supervisory system to monitor for wires to third-party accounts. From October 2011 to October 2013, Scottrade did not obtain any customer confirmations for third-party wire transfers of less than $200,000, and Scottrade failed to ensure that the appropriate personnel obtained confirmations for third-party wire transfers of between $200,000 and $500,000. During that period, the firm processed over 17,000 third-party wire transfers totaling more than $880 million.[15]

33. In addition, a hacker was recently sentenced to prison for hacking into retail brokerage accounts and making unauthorized trades from online accounts at Scottrade and other brokerage accounts:

> A Russian national living in New York, Petr Murmylyuk, was sentenced to 30 months in prison in January for hacking into retail brokerage accounts and making unauthorized trades from online accounts at Scottrade, E*Trade Financial ETFC, +2.74% , Fidelity Investments, Charles Schwab SCHW, +2.25% and other brokerages. He and his co-conspirators made trades in victim accounts to move the prices of holdings in accounts they had opened using stolen identities, causing about $1 million in losses, according to the Federal Bureau of Investigation. The court ordered Murmylyuk to pay about $500,000 in restitution.[16]

---

[15] Press Release, FINRA Fines Morgan Stanley Smith Barney and Scottrade a Total of $950,000 for Failing to Supervise the Transmittal of Customer Funds to Third-Party Accounts, (June 22, 2015) https://www.finra.org/newsroom/2015/finra-fines-mssb-scottrade-950k-failing-supervise-transmittal-customer-funds.

[16] Priya Anand, Was your brokerage account hacked? Here's how to know, (Oct. 9, 2014), http://www.marketwatch.com/story/was-your-brokerage-account-hacked-heres-how-to-know-

34. Moreover, Scottrade knew or should have known it was susceptible to data breaches in light of the recent rise in massive security breaches on the internet and the fact that the information contained on Scottrade's network is particularly sensitive.

35. Despite prior warnings that its security measures were inadequate, Scottrade failed to heed those warnings and instead put its customers at risk.

V. PLAINTIFFS AND THE CLASS SUFFERED HARM

36. At all relevant times, Scottrade had a duty to, and represented to Plaintiffs and members of the Class that it would properly secure the personal and financial information in its network and act reasonably to prevent the foreseeable harms to Plaintiffs and the Class which would naturally result from data theft.

37. The damage that results from data theft is severe. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data, such as social security numbers, to open financial accounts, receive government benefits and incur charges and credit in a person's name.[17] As stated in the GAO Report, this type of identity theft is the most harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

38. The GAO Report also notes that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."

39. The Federal Trade Commission ("FTC") also recognizes the damage and costs incurred by identity theft victims. According to the FTC, identity theft victims must spend

---

2014-07-25.

[17] http:///www.gao.gov/new.items/d07737.pdf.

countless hours and large amounts of money repairing the impact to their good name and credit record.[18] Identity thieves use stolen personal information, such as social security numbers, for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[19]

40. In addition to emptying out a victim's bank account, identity thieves may commit various other frauds, such as: (1) obtaining a driver's license or official identification card in the victim's name; (2) using the victim's name and social security number to obtain government benefits; (3) filing a fraudulent tax return using the victim's information; (4) obtaining a job using the victim's social security number; (5) renting a home using the victim's information; (6) receiving medical services in the victim's name; and/or (7) providing the victim's information to the police during an arrest.[20]

41. When personal information is compromised, a victim may not see signs of identity theft until years later. According to the GAO Report:

> law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

42. Personal information is a valuable commodity to identity thieves, so much so that criminals often trade the information on the "cyber black-market" for a number of years. On the "cyber black-market," stolen private information gets posted, making the information publicly

---

[18] FTC Identity Theft Website, www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

[19] *Id.*

[20] *Id.*

available. In one study, researchers found hundreds of websites were blocked by Google's safeguard filtering mechanism-the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[21]

43. As a result of Scottrade's inadequate security measures, Plaintiffs and the class have suffered damage, including: (a) time, effort, and out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; (b) credit, debt, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of the breach; (c) the value of their time and resources spent mitigating the identity theft and/or fraud; (d) the cost and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards; and (e) the financial losses for any unauthorized charges by identity thieves.

44. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges are discovered and occur.

CLASS ACTION ALLEGATIONS

45. Plaintiffs bring this action pursuant to Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3) individually and on behalf of the class, defined as follows:

> All current and former customers of Scottrade in the United States (including its territories and the District of Columbia) whose personal or financial information was compromised as a result of the data breach announced on October 2, 2015 (the "National Class").

46. Plaintiffs also bring this action on behalf of the following subclasses:

[21] http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/

> All current and former customers of Scottrade in New York whose personal or financial information was compromised as a result of the data breach announced on October 2, 2015 (the "New York Subclass").
>
> All current and former customers of Scottrade in New Jersey whose personal or financial information was compromised as a result of the data breach announced on October 2, 2015 (the "New Jersey Subclass").
>
> All current and former customers of Scottrade in California whose personal or financial information was compromised as a result of the data breach announced on October 2, 2015 (the "California Subclass").

47. The National Class, New York Subclass, New Jersey Subclass, and California Subclass are collectively referred to as the "Class," unless specifically indicated otherwise.

48. Excluded from the Class are the following individuals and/or entities: Scottrade and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Scottrade has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, division, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

49. Plaintiffs reserve the right to modify or amend the definition of the Class after they have had an opportunity to conduct discovery.

50. ***Numerosity. Rule 23(a)(1).*** The Class is so numerous that joinder of all members is impracticable. Plaintiffs are informed and believe that the proposed Class contains at least thousands of customers, as Scottrade has confirmed that the number of separate individuals whose private financial data has been compromised as a result of the Security Breach is approximately 4.6 million. The number of Class members is unknown to the Plaintiffs but could be discerned from the records maintained by Scottrade.

51. ***Existence of Common Questions of Law and Fact. Rule 23(a)(2).*** This action involves substantial questions of law and fact common to all members of the Class, which include, but are not limited to, the following:

a. Whether Scottrade failed to employ reasonable and industry-standard measures to secure and safeguard its customers' personal and financial data;

b. Whether Scottrade failed to properly implement and maintain its purported security measures to protect its customers' personal and financial data;

c. Whether Scottrade's security failures resulted in the unauthorized breach of Scottrade's network containing customers' personal and financial information;

d. Whether Scottrade misrepresented that its customers' personal and financial information was secure;

e. Whether Scottrade was negligent in failing to properly secure and protect its customers' personal and financial information;

f. Whether Scottrade's conduct violated New York General Business Law § 349;

g. Whether Scottrade's conduct violated the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-2, *et seq.*;

h. Whether Scottrade's conduct violated the California Civil Code § 1798.80 *et seq.*;

i. Whether Scottrade's conduct violated California's Unfair Competition Law;

j. Whether Plaintiffs and other members of the Class are entitled to injunctive relief; and

k. Whether Plaintiffs and other members of the Class are entitled to damages and the measure of such damages.

52. ***Typicality. Rule 23(a)(3).*** Plaintiffs' claims are typical of the claims of the

members of the Class. Plaintiffs and the members of the Class were damaged by the same unreasonable conduct of Scottrade.

53. ***Adequacy. Rule 23(a)(4).*** Plaintiffs will fairly and adequately protect the interests of the members of the Class. Plaintiffs have retained counsel experienced in complex class action litigation and Plaintiffs intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class.

54. ***Injunctive Relief. Rule 23(b)(2).*** Scottrade's actions complained of herein are uniform as to all members of the Class. Scottrade has acted or refused to act on grounds that apply generally to the Class, so that final injunctive relief as requested herein is appropriate respecting the Class as a whole.

55. ***Predominance and Superiority of Class Action. Rule 23(b)(3).*** Questions of law or fact common to the Class predominate over any questions affecting only individual members and a class action is superior to other methods for the fast and efficient adjudication of this controversy, for at least the following reasons:

a. Absent a class action, members of the Class as a practical matter will be unable to obtain redress, Scottrade's violations of its legal obligations will continue without remedy, and additional customers will be harmed;

b. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions;

c. When the liability of Scottrade has been adjudicated, the Court will be able to determine the claims of all members of the Class;

d. A class action will permit an orderly and expeditious administration of each Class member's claims and foster economies of time, effort, and expense;

e. A class action regarding the issues in this case does not create any problems of manageability;

f. Scottrade has acted on grounds generally applicable to the members of the Class, making class-wide monetary relief appropriate.

FIRST CLAIM FOR RELIEF

BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

56. Plaintiffs repeat and re-allege all previous allegations as if fully set forth herein.

57. By virtue of Scottrade's possession, custody and/or control of Plaintiffs' and Class members' personal and private information, and Scottrade's duty to properly monitor and safeguard such information, the Defendant was (and continues to be) in a confidential, special and/or fiduciary relationship with Plaintiffs and the Class. As fiduciaries, the Defendant owes (and continues to owe) to Plaintiffs and Class members:

a. The commitment to deal fairly and honestly;

b. The duties of good faith and undivided loyalty; and

c. Integrity of the strictest kind. The Defendant was (and continues to be) obligated to exercise the highest degree of care in carrying out its responsibilities to Plaintiffs and Class members under such confidential, special and/or fiduciary relationships.

58. Scottrade breached its fiduciary duties to Plaintiffs and the Class by, *inter alia*, improperly storing, monitoring and/or safeguarding the Plaintiffs' and Class members' personal and private information.

59. Scottrade breached its fiduciary duties to Plaintiffs and the Class by its wrongful actions described above. Defendant willfully and wantonly breached its fiduciary duties to Plaintiffs and the Class or, at the very least, committed these breaches with conscious indifference

and reckless disregard of its rights and interests. The Defendant's wrongful actions constitute breach of fiduciary duty at common law.

SECOND CLAIM FOR RELIEF

NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

60. Plaintiffs repeat and re-allege all previous allegations as if fully set forth herein.

61. Scottrade came into possession, custody and/or control of confidential personal and financial information of Plaintiffs and Class members.

62. In collecting the personal information of its current and former customers, Scottrade owed Plaintiffs and the members of the Class a duty to exercise reasonable care in safeguarding, keeping private, and protecting such information from being accessed by and disclosed to third parties.

63. Scottrade had a duty to, among other things, maintain and test its security systems and take other reasonable security measures to protect and adequately secure the personal data of Plaintiffs and the Class from unauthorized access and use.

64. Scottrade was aware that by taking such sensitive personal information from its customers that it had a responsibility to take reasonable security measures to protect the data from being stolen and easily accessed.

65. Scottrade also had a duty to exercise reasonable care by timely notifying Plaintiffs and the Class of an authorized disclosure of their confidential personal or financial information.

66. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' personal and financial information within Defendant's possession.

67. Defendant, through its actions and/or omissions, unlawfully breached its duty to

Plaintiffs and the Class by failing to exercise reasonable care by failing to have appropriate procedures in place to detect and prevent the dissemination of Plaintiffs' personal and financial information.

68. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to timely disclose that the personal and financial information within Defendant's possession had been released to unauthorized persons.

69. Defendant's negligent and wrongful breach of its duties owed to Plaintiffs and the Class proximately caused Plaintiffs' and Class members' personal and financial information to be compromised.

70. Plaintiffs seek the award of actual damages on behalf of the Class.

THIRD CLAIM FOR RELIEF

BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Class)

71. Plaintiffs repeat and re-allege all previous allegations as if fully set forth herein.

72. Plaintiffs and the Class were parties to actual or implied contracts with Scottrade that required Scottrade to properly safeguard their personal and financial information from theft, compromise and/or unauthorized disclosure.

73. Scottrade solicited Plaintiffs and the Class to sign up with Scottrade and to provide their personal and financial information. Plaintiffs and the Class later paid fees to Scottrade based on Scottrade's express representations concerning the safeguarding and protection of personal and financial information.

74. Plaintiffs and the Class fully performed their obligations under their contracts with Scottrade.

75. Scottrade breached its agreements with Plaintiffs and the Class by failing to properly safeguard their personal and financial information from theft, compromise and/or unauthorized disclosure. The Defendant's wrongful conduct constitutes breach of contract.

FOURTH CAUSE OF ACTION

NEW YORK GENERAL BUSINESS LAW § 349
(On Behalf of Plaintiff Stern and the New York Subclass)

76. Plaintiff Stern repeats and re-alleges all previous allegations as if fully set forth herein.

77. As fully alleged above, Scottrade engaged in unfair and deceptive acts and practices in violation of Section 349 of the New York General Business Law ("GBL").

78. Reasonable consumers would be misled by Defendant's misrepresentations and/or omissions concerning the security of their personal information, because they understand that national brokerage companies that take personal and financial information from customers will properly safeguard that private information in a manner consistent with industry standards and practices.

79. Scottrade did not inform its customers that it failed to properly safeguard their personal and financial information, thus misleading Plaintiff Stern and the New York Subclass in violation of GBL § 349. Such misrepresentations were material because Plaintiff Stern and the New York Subclass entrusted Scottrade with their private information.

80. As a direct and proximate result of Scottrade's violations, Plaintiff Stern and the New York Subclass suffered injury in fact and loss, including loss of time and money monitoring their finances for future fraud and other damages.

81. Plaintiff Stern and the New York Subclass seek injunctive relief in the form of an order: (a) compelling Scottrade to institute appropriate data collection and safeguarding methods

and policies with regard to consumer information; and (b) compelling Scottrade to provide detailed and specific disclosure of what types of personal and financial information have been compromised as a result of the data breach.

82. Plaintiff Stern seeks attorney's fees and damages to the fullest extent permitted under GBL § 349(a).

FIFTH CAUSE OF ACTION

VIOLATION OF NEW JERSEY CONSUMER FRAUD ACT, N.J.S.A §56:8-2, *et. seq.* (On Behalf of Plaintiff Soffer and the New Jersey Subclass)

83. Plaintiff Soffer repeats and re-alleges all previous allegations as if fully set forth herein.

84. The New Jersey Consumer Fraud Act ("NJCFA") protects consumers against "any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise . . . ." N.J.S.A. § 56:8-2.

85. In enacting the Identity Theft Prevention Act, which among other things, amended the New Jersey Consumer Fraud Act, the New Jersey Legislature found that "[i]dentity theft is an act that violates the privacy of our citizens and ruins their good names: victims can suffer restricted access to credit and diminished employment opportunities, and may spend years repairing damage to credit histories." N.J.S.A. §56:1-45.

86. Scottrade violated the NJCFA by affirmatively representing that Plaintiff Soffer and the New Jersey Subclass's personal and financial information would be collected and stored securely. Scottrade also engaged in unlawful conduct in violation of the NJCFA by making knowing and intentional omissions regarding the inadequacy of its data security systems.

87. Defendant knew or should have known that its data security systems and procedures were inadequate. Scottrade did not fully and truthfully disclose to its customers the inadequate nature of its data security systems, omitting material facts that it was under a duty to disclose to Plaintiff Soffer and the New Jersey Subclass.

88. Plaintiff Soffer and the New Jersey Subclass reasonably expected that their personal and financial information would be securely collected and maintained such that the data breach would not occur.

89. As a result, Plaintiff Soffer and the New Jersey Subclass were fraudulently induced to sign up with Scottrade and provide personal and financial information to Defendant without knowledge of Defendant's inadequate data security systems and procedures. The facts that Defendant concealed were solely within its possession.

90. Defendant intended for Plaintiff Soffer and the New Jersey Subclass to rely on its acts of concealment and omissions so that they would use Scottrade's services.

91. If Plaintiff Soffer and members of the New Jersey Subclass knew about Defendant's inadequate data security and procedures, they would not have used Scottrade's services or would not have provided their personal and/or financial information to Scottrade.

92. Defendant's conduct caused Plaintiff Soffer and the New Jersey Subclass to suffer an ascertainable loss by having their personal and financial information compromised.

SIXTH CAUSE OF ACTION

FAILURE TO EXPEDIENTLY NOTIFY CUSTOMERS IN VIOLATION OF THE NEW JERSEY CONSUMER FRAUD ACT, N.J.S.A. 56:8-2, *et seq.* (On Behalf of Plaintiff Soffer and the New Jersey Subclass)

93. Plaintiff Soffer repeats and re-alleges all previous allegations as if fully set forth herein.

94. As stated above, the New Jersey Consumer Fraud Act provides that it is "an unlawful practice and a violation of P.L. 1960 c. 39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate" Sections 56:8-161-164 of that Act.

95. Section 56:8-163 of the New Jersey Consumer Fraud Act requires that a business conducting business in New Jersey:

> shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

N.J.S.A. § 56:8-163.

96. The New Jersey Consumer Fraud Act defines a breach of security as follows:

> "Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

N.J.S.A. § 56:8-161.

97. Scottrade's data breach constitutes a breach of security.

98. Scottrade's disclosure regarding the breach of security to Plaintiff Soffer and the new Jersey Subclass was delayed and not made in the most expedient time possible.

99. As a result of the foregoing, Plaintiff Soffer and the New Jersey Subclass suffered and will continue to suffer ascertainable losses and other damages, and are entitled to treble damages as provided by N.J.S.A. § 56:18-19.

SEVENTH CAUSE OF ACTION

CALIFORNIA CIVIL CODE §1798.80, et seq.
(On Behalf of Plaintiff Jenani and the California Subclass)

100. Plaintiff Jenani repeats and re-alleges all previous allegations as if fully set forth herein.

101. The events alleged herein constitute a "breach of the security system" of Scottrade within the meaning of California Civil Code §1798.82.

102. The information lost, disclosed, or intercepted during the events alleged herein constitute unencrypted "personal information" within the meaning of California Civil Code §§1798.80(e) and 1798.82(h).

103. Scottrade failed to implement and maintain reasonable or appropriate security procedures and practices to protect customers' personal and financial information. Upon information and belief, Scottrade failed to employ industry standard security measures, best practices or safeguards with respect to customers' personal and financial information.

104. Scottrade failed to disclose the breach of security to its network using means and methods to reach all affected customers, in the most expedient time possible, and without unreasonable delay after it knew or reasonably believed that customers' personal and financial data had been compromised.

105. The breach of the personal information of millions of accounts of Scottrade customers constituted a "breach of the security system" of Scottrade pursuant to Civil Code section 1798.82(g).

106. By failing to implement reasonable measures to protect its customers' personal data, Scottrade violated Civil Code section 1798.81.5.

107. By failing to promptly notify all affected Scottrade customers that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, Scottrade violated Civil Code section 1798.82 of the same title in a manner that would reach all affected customers.

108. By violating Civil Code sections 1798.81.5 and 1798.82, Scottrade "may be enjoined" under Civil Code section 1798.84(e).

109. Accordingly, Plaintiff Jenani requests that the Court enter an injunction requiring Scottrade to implement and maintain reasonable security procedures to protect customers' data in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Scottrade, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Scottrade's systems on a periodic basis; (2) ordering that Scottrade engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Scottrade audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Scottrade, consistent with industry standard practices, conduct regular database scanning and security checks; (5) ordering that Scottrade, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (6) ordering Scottrade to meaningfully educate its customers about the threats they face as a result of the loss of their personal and financial information to third parties, as well as the steps Scottrade customers must take to protect themselves.

110. Plaintiff Jenani further requests that the Court require Scottrade to (1) identify and notify all members of the Class who have not yet been informed of the data breach; and (2) notify affected customers of any future data breaches by email, text, and pre-recorded phone calls within 24 hours of Scottrade's discovery of a breach or possible breach and by mail within 72 hours.

111. As a result of Scottrade's violation of Civil Code sections 1798.81, 1798.81.5, and 1798.82, Plaintiff Jenani and members of the California Subclass have and will incur economic damages relating to time and money spent remedying the breach, expenses for bank fees associated with the breach, late fees from automated billing services associated with the breach, as well as the costs of credit monitoring and purchasing credit reports.

112. Plaintiff Jenani, individually and on behalf of the members of the California Subclass, seek all remedies available under Civil Code section 1798.84, including, but not limited to: (a) damages suffered by members of the California Subclass; and (b) equitable relief. Plaintiff Jenani, individually and on behalf of the California Subclass, also seeks reasonable attorneys' fees and costs under applicable law.

EIGHTH CAUSE OF ACTION

CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL")
(On Behalf of Plaintiff Jenani and the California Subclass)

113. Plaintiff Jenani repeats and re-alleges all previous allegations as if fully set forth herein.

114. Beginning at an exact date unknown, but at least since October 1, 2015, Scottrade has committed and continues to commit acts of unfair competition, as defined by California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, et seq.

115. As specifically alleged herein, Scottrade's acts, practices, omissions and nondisclosures violate Cal. Civ. Code §§ 1572, 1573, 1709, 1711, 1798.80 et seq., and the common law. Consequently, Scottrade's acts, practices, omissions, and nondisclosures, as alleged herein, constitute unlawful acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200.

116. Scottrade's acts, practices, omissions, and nondisclosures threaten a continued violation of Cal. Civ. Code §§ 1709, 1711, 1798.80 et seq., and the common law, violate the policy and spirit of such laws, and otherwise significantly harm consumers.

117. Scottrade's acts, practices, omissions, and nondisclosures are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers. The harm to Plaintiff Jenani, the California Subclass, and members of the general public substantially outweighs any benefits of Scottrade's conduct. Furthermore, there were reasonably available alternatives to further Scottrade's legitimate business interests, including using the best practices to protect the personal and financial information other than Scottrade's wrongful conduct described herein. Consequently, Scottrade's acts, practices, omissions, and nondisclosures constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200.

118. Scottrade's acts, practices, omissions and nondisclosures, as alleged herein, are likely to deceive, and did deceive, Plaintiff Jenani, the California Subclass, and members of the general public, and consequently constitute "fraudulent" acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200. Scottrade's conduct was likely to deceive reasonable consumers.

119. Scottrade violated the UCL by accepting and storing personal and financial information of Plaintiff Jenani and the California Subclass and then failing to take reasonable steps to protect it. In violation of industry standards, best practices, and reasonable consumer expectations, Scottrade failed to safeguard personal and financial information and failed to tell consumers that it did not have reasonable and best practices, safeguards and data security in place to protect their personal and financial information.

120. As a result of Scottrade's conduct, Plaintiff Jenani and the California Subclass have suffered damage and been harmed by, among other things: (a) the interception, loss, and disclosure of their personal and financial information; and (b) making purchases from Scottrade that they otherwise would not have made or would have paid less for had they known their personal information was at risk of disclosure. In addition, Plaintiff Jenani and the California Subclass have suffered harm through the expenditure of time and resources in connection with: (a) discovering and assessing fraudulent or unauthorized charges; (b) contesting fraudulent or unauthorized charges; (c) adjusting automatic or other billing instructions; and (d) obtaining credit monitoring and identity theft protection.

121. Plaintiff Jenani and the California Subclass seek injunctive relief, restitution and/or disgorgement, and any further relief that the Court deems proper. In addition, Plaintiff Jenani seeks reasonable attorneys' fees and prays for the relief set forth below.

NINTH CAUSE OF ACTION
BAILMENT
(On Behalf of Plaintiffs and the Class)

122. Plaintiffs repeat and re-allege all previous allegations as if fully set forth herein.

123. Plaintiffs' and the Class's personal and financial information is their personal property, which they delivered to Scottrade for the sole and specific purpose of paying for services from Scottrade.

124. Defendant accepted Plaintiffs' and the Class's personal information. As bailee, the Defendant owed a duty to Plaintiffs and the Class and, in fact, had an express and/or implied contract with them, to use their personal and financial information only for that period of time necessary to complete the services by Scottrade.

125. Scottrade breached its duty and/or express and/or implied contracts with the Plaintiffs and Class members by, *inter alia*, improperly storing and inadequately protecting Plaintiffs' and the Class's personal information from theft, compromise and/or unauthorized disclosure, which directly and/or proximately caused the Plaintiffs and the Class to suffer damages.

126. Scottrade's wrongful actions constitute breaches of its duty to (and/or express and/or implied contracts with) the Plaintiffs and the Class arising from the bailment.

WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully request that the Court enter judgment in its favors as follows:

A. Determine that this action be maintained as a class action pursuant to Federal Rule of Civil Procedure 23(a), (b)(2) and (b)(3);
B. Direct that reasonable notice of this action, as provided by Federal Rule of Civil Procedure 23(c)(2), be given to the Class;
C. Appoint Plaintiff Stern as class representative for the New York Subclass, appoint Plaintiff Soffer as class representative for the New Jersey Subclass, appoint Plaintiff Jenani as class representative for the California Subclass and appoint Plaintiffs' counsel as counsel for the Class;
D. Enter judgment against Scottrade and in favor of the Plaintiffs and the Class;
E. Order Scottrade to pay for not less than three years of credit and identity theft monitoring services for Plaintiffs and the Class;
F. Award all compensatory and statutory damages to the Plaintiffs and the Class in an amount to be determined at trial;

G. Award punitive damages, including treble and/or exemplary damages, in an appropriate amount;

H. Award the Plaintiffs and the Class the costs incurred in this action together with reasonable attorneys' fees and expenses, including any necessary expert fees as well as pre-judgment and post-judgment interest; and

I. Grant such other and further relief as is necessary to correct for the effects of Scottrade's unlawful conduct and as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs, on behalf of themselves and the Class, demand a trial by jury on all issues so triable.

DATED: October 30, 2014

Respectfully submitted,

LEVI & KORSINSKY LLP

By: */s/ Shannon L. Hopkins*

Shannon L. Hopkins (SH1887)
shopkins@zlk.com
Nancy A. Kulesa (NK2015)
nkulesa@zlk.com
Stephanie A. Bartone
sbartone@zlk.com
733 Summer Street, Suite 304
Stamford, CT 06901
Telephone: (212) 363-7500
Facsimile: (212) 363-7171